

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-7352

(P2002-7352A)

(43)公開日 平成14年1月11日(2002.1.11)

(51)Int.Cl.	識別記号	P I	キーワード(参考)
G 0 6 F 15/00	3 9 0	G 0 6 F 15/00	3 9 0 F 5 B 0 8 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A 5 J 1 0 4
			6 7 3 D

調査請求 未請求 請求項の数7 O L (全 15 頁)

(21)出願番号 特願2000-191347(P2000-191347)

(22)出願日 平成12年6月26日(2000.6.26)

(71)出願人 000005234

富士電機株式会社

神奈川県川崎市川崎区田辺新田1番1号

(72)発明者 西田 廣治

神奈川県川崎市川崎区田辺新田1番1号

富士電機株式会社内

(74)代理人 100074069

弁理士 大曾 義之

Fターム(参考) 5B085 AE23 AE25 AE26 AE27 AE29

5J104 AA07 KA01 KA16 KA17 KA18

KA19 MA02 PA07

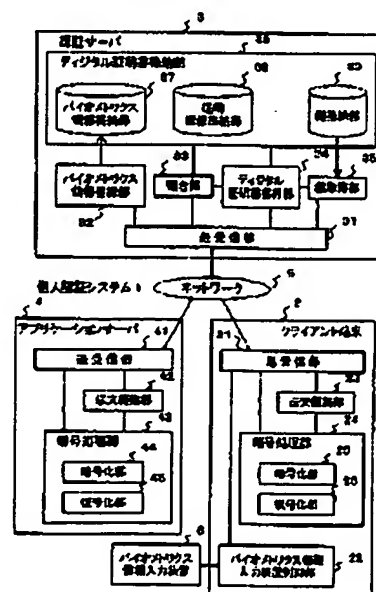
(54)【発明の名称】 個人認証システムおよび個人認証方法

(57)【要約】

【課題】 認証の安全性を高め、デジタル証明書を認証サーバからダウンロードする場合もIDやパスワード等の入力無しに自動的に認証サーバからデジタル証明書をダウンロード可能にすることが課題である。

【解決手段】 アプリケーションサービスを提供するアプリケーションサーバとユーザが使用するクライアント端末とユーザを認証する認証サーバとが互いにネットワークを介して接続される個人認証システムにおける個人認証方法であって、クライアント端末を操作するユーザのバイOMETRICS情報を取得して認証サーバに送信し、予め認証サーバのデジタル証明書内に格納されたバイOMETRICS情報と照合してユーザが正規なユーザであるか否かを判断し、この判断により正規なユーザである場合は、伝文を暗号化して伝送する。

本発明の個人認証システムの概略ブロック図



【特許請求の範囲】

【請求項1】 アプリケーションサーバを提供するアプリケーションサーバとユーザが使用するクライアント端末と前記ユーザを認証する認証サーバとが互いにネットワークを介して接続される個人認証システムにおける個人認証方法であって、

前記クライアント端末が、前記クライアント端末を操作するユーザのバイOMETRICS情報を取得して前記認証サーバに送信し、

前記取得したバイOMETRICS情報を受信した前記認証サーバが、正規のユーザであることを示すデジタル証明書内に予め格納しているバイOMETRICS情報と照合することにより、前記ユーザが正規のユーザであるか否かを判断し、

前記判断により正規なユーザである場合は、前記認証サーバが、前記クライアント端末に対して前記デジタル証明書を発行し、

前記デジタル証明書を受信した前記クライアント端末が前記アプリケーションサーバのデジタル証明書入手し、前記アプリケーションサーバに対して、前記クライアントのデジタル証明書によりデジタル署名を付し、前記アプリケーションサーバのデジタル証明書内の暗号化鍵により暗号化した伝文を送信することを特徴とする個人認証方法。

【請求項2】 前記アプリケーションサーバが、前記ユーザ及び前記アプリケーションサーバのデジタル証明書を取得し、受信した前記伝文を前記ユーザ及び前記アプリケーションサーバのデジタル証明書内の復号化鍵により復号化することを特徴とする請求項1に記載の個人認証方法。

【請求項3】 前記予め格納しているバイOMETRICS情報は、前記クライアント端末が、前記クライアント端末を操作するユーザのバイOMETRICS情報を取得して前記認証サーバに送信し、前記取得したバイOMETRICS情報を受信した前記認証サーバが、正規のユーザであることを示すデジタル証明書内に登録することを特徴とする請求項1または2に記載の個人認証方法。

【請求項4】 前記デジタル証明書がバイOMETRICS認証に対応していない場合に、前記予め格納されたバイOMETRICS情報は、前記認証サーバが有する変換テーブルに、ユーザのID情報と対応させて格納されていることを特徴とする請求項1に記載の個人認証方法。

【請求項5】 前記バイOMETRICS情報は、指紋情報、虹彩情報、声紋情報、網膜パターン情報、掌脈情報またはDNA情報であることを特徴とする請求項1乃至4の何れか1項に記載の個人認証方法。

【請求項6】 アプリケーションサーバを提供するアプリケーションサーバとユーザが使用するクライアント端末とが互いにネットワークを介して接続される個人認証システムであって、

前記ネットワークに接続され、前記ユーザを認証する認証サーバを備え、

前記認証サーバは、

正規なアプリケーションサーバとしてあるいは正規なユーザとして登録してあることを証明する所定のデジタル証明書と、指紋情報、虹彩情報、声紋情報、網膜パターン情報、掌脈情報またはDNA情報であるバイOMETRICS情報を格納するバイOMETRICS情報格納部と、前記デジタル証明書に記されないデジタル証明項目の情報を格納する証明情報格納部と、暗号化鍵または復号化鍵を格納する鍵格納部とを有するデジタル証明書格納部と、

受信したバイOMETRICS情報と前記バイOMETRICS情報格納部に格納されたバイOMETRICS情報とを照合する照合部と、

前記デジタル証明書を発行するデジタル証明書発行部と、

前記暗号化鍵または前記復号化鍵を取得する鍵取得部とを備え、

20 前記クライアント端末は、

前記バイOMETRICS情報を読み込むためのバイOMETRICS情報入力装置を制御するバイOMETRICS情報入力装置制御部と、

前記アプリケーションサーバへ伝送する伝文を編集する伝文編集部と、

前記伝文編集部が編集した伝文を暗号化し、前記アプリケーションサーバから伝送されてきた伝文を復号化する暗号化処理部とを備え、

前記アプリケーション端末は、

30 前記クライアント端末へ伝送する伝文を編集する伝文編集部と、

前記伝文編集部が編集した伝文を暗号化し、前記クライアント端末から伝送されてきた伝文を復号化する暗号化処理部とを備えることを特徴とする個人認証システム。

【請求項7】 前記認証サーバは、さらに、バイOMETRICS情報登録部を備えることを特徴とする請求項6に記載の個人認証システム。

【発明の詳細な説明】

【0001】

40 【発明の属する技術分野】本発明は、アプリケーションサーバとクライアント端末間の暗号文伝送に関し、特に、指紋、声紋等のバイOMETRICS情報によりクライアント端末を使用するユーザを認証する個人認証システムおよび個人認証方法に関する。

【0002】

【従来の技術】現在、通信回線のインフラが盛んになり、コンピュータをはじめとする情報機器は、通信回線を介して相互に接続されている。そして、我々ユーザは、情報機器を用い、通信回線を介して様々なサービス50 を利用することができるようになってきた。

【0003】サービスの種類が増える一方で、金銭やプライバシーが絡むサービスにおいては、利用者が本人であることを確認することが必要である。また、自動的にパスワードを発見するプログラムを作成できる等、利用者に成りすまそうとする犯罪者にとっても好都合な環境が整いつつある。

【0004】そこで、指紋、声紋等のバイオメトリクス情報を用いた照合は、管理や記憶の容易さや本人認証の正確さから、パスワード等に代わる方法として実現されている。

【0005】従来は、アプリケーションサーバとクライアント端末間を公開鍵方式で暗号文伝送をするに当たり、アクセス権限を持ったユーザであるか否かの認証を指紋、虹彩、声紋、網膜パターン、筆跡、DNAなどのバイオメトリクス情報で認証を行う場合、ユーザが使用するクライアント端末内または、クライアント端末に接続されバイオメトリクス情報を入力するバイオメトリクス情報入力装置で照合をおこなっていた。

【0006】さらに、認証サーバから証明書をダウンロードする際は、そのためのIDやパスワードを入力していた。また、特開平11-195120号公報には、端末装置における電子文書の編集時に、カーソルが押印エリア（またはサインエリア）内に入ると、指紋検出部が編集者の指紋を検出し、その検出された指紋情報をホスト装置に送信する。そして、ホスト装置において、上記指紋情報が照合されることによりユーザ認証が行われ、同時に、照合された指紋情報と共に予め登録されている印章データ（またはサインデータ）が端末装置に返送される。端末装置では、その返送された印章データが押印エリアに書き込まれることにより、編集した電子文書に対する署名が実現される技術が開示されている。

【0007】

【発明が解決しようとする課題】しかしながら、従来の個人認証システムまたは個人認証方法においては、バイオメトリクス情報で認証を行う場合、ユーザが使用するクライアント端末内または、クライアント端末に接続されバイオメトリクス情報を入力するバイオメトリクス情報入力装置で照合をおこなっていたため、照合の妥当性をアプリケーションサーバが確認できず、安全性の上で不十分であるという問題があった。

【0008】本発明の課題は、認証の安全性を高め、デジタル証明書を認証サーバからダウンロードする場合もIDやパスワード等の入力無しに自動的に認証サーバからデジタル証明書をダウンロード可能とする個人認証システムおよび個人認証方法を提供することである。

【0009】

【課題を解決するための手段】本発明は、上記課題を解決するため、下記のような構成を採用した。すなわち、本発明の一態様によれば、本発明の個人認証方法は、アプリケーションサーバを提供するアプリケーションサ

サーバとユーザが使用するクライアント端末と上記ユーザを認証する認証サーバとが互いにネットワークを介して接続される個人認証システムにおける個人認証方法であって、上記クライアント端末が、上記クライアント端末を操作するユーザのバイオメトリクス情報を取得して上記認証サーバに送信し、上記取得したバイオメトリクス情報を受信した上記認証サーバが、正規のユーザであることを示すデジタル証明書内に予め格納しているバイオメトリクス情報と照合することにより、上記ユーザが正規のユーザであるか否かを判断し、上記判断により正規なユーザである場合は、上記認証サーバが、上記クライアント端末に対して上記デジタル証明書を発行し、上記デジタル証明書を受信した上記クライアント端末が、上記アプリケーションサーバに対して、デジタル証明書によりデジタル署名を付し、あらかじめ入手したアプリケーションサーバのデジタル証明書内の暗号化鍵により暗号化した伝文を送信することを特徴とする。

【0010】また、好適には、本発明の個人認証方法は、上記アプリケーションサーバが、上記ユーザのデジタル証明書を取得し、受信した上記デジタル署名をデジタル証明書内の復号化鍵により復号化し、上記伝文を上記アプリケーションサーバのデジタル証明書内の復号化鍵により復号化する。

【0011】また、好適には、本発明の個人認証方法は、上記予め格納しているバイオメトリクス情報が、上記クライアント端末によって、上記クライアント端末を操作するユーザのバイオメトリクス情報を取得されて上記認証サーバに送信され、上記取得したバイオメトリクス情報を受信した上記認証サーバによって、正規のユーザであることを示すデジタル証明書内に登録される。

【0012】また、好適には、本発明の個人認証方法は、上記デジタル証明書がバイオメトリクス認証に対応していない場合に、上記予め格納されたバイオメトリクス情報が、上記認証サーバが有する変換テーブルに、ユーザのID情報と対応させて格納されている。

【0013】また、好適には、本発明の個人認証方法は、上記バイオメトリクス情報が、指紋情報、虹彩情報、声紋情報、網膜パターン情報、筆跡情報またはDNA情報である。

【0014】また、本発明の一態様によれば、本発明の個人認証システムは、アプリケーションサーバを提供するアプリケーションサーバとユーザが使用するクライアント端末とが互いにネットワークを介して接続される個人認証システムであって、上記ネットワークに接続され、上記ユーザを認証する認証サーバを備え、上記認証サーバが、正規なアプリケーションサーバとしてあるいは正規なユーザとして登録してあることを証明する（例えば、WebブラウザがサポートするSSL（Secure Socket Layer）プロトコル、電子商

取引用のSET (Secure Electronic Transactions) プロトコル、電子メール用のS/MIME (Secure Multipurpose Internet Mail Extensions) などのように) ITU-T (International Telecommunication Union Telecommunication standardization: 国際電気通信連合電気通信標準) により勧告されたX. 509で定められたデジタル証明書と、指紋情報、虹彩情報、声紋情報、網膜パターン情報、掌脈情報またはDNA情報であるバイオメトリクス情報を格納するバイオメトリクス情報格納部と、前記デジタル証明書に記されないデジタル証明項目の情報を格納する証明情報格納部と、暗号化鍵または復号化鍵を格納する鍵格納部とを有するデジタル証明書格納部と、受信したバイオメトリクス情報と上記バイオメトリクス情報格納部に格納されたバイオメトリクス情報とを照合する照合部と、上記デジタル証明書を発行するデジタル証明書発行部と、上記暗号化鍵または上記復号化鍵を取得する鍵取得部とを備え、上記クライアント端末が、上記バイオメトリクス情報を読み込むためのバイオメトリクス情報入力装置を制御するバイオメトリクス情報入力装置制御部と、上記アプリケーションサーバへ伝送する伝文を編集する伝文編集部と、上記伝文編集部が編集した伝文を暗号化し、上記アプリケーションサーバから伝送されてきた伝文を復号化する暗号化処理部とを備え、上記アプリケーション端末が、上記クライアント端末へ伝送する伝文を編集する伝文編集部と、上記伝文編集部が編集した伝文を暗号化し、上記クライアント端末から伝送されてきた伝文を復号化する暗号化処理部とを備えることを特徴とする。

【0015】また、好適には、本発明の個人認証システムは、上記認証サーバが、さらに、バイオメトリクス情報登録部を備える。

【0016】

【発明の実施の形態】以下、本発明の実施の形態を、図面を参照しながら詳細に説明する。図1は、本発明の個人認証システムの機能ブロック図である。

【0017】図1において、個人認証システム1は、アプリケーションサーバを提供するアプリケーションサーバ4と、ユーザが使用するクライアント端末2と、上記ユーザまたは上記アプリケーションサーバを認証する認証サーバ3とが互いにネットワーク5を介して接続され、クライアント端末2には、指紋、虹彩、声紋、網膜パターン、掌脈、DNAなどのバイオメトリクス情報を入力するためのバイオメトリクス情報入力装置6が接続されている。

【0018】アプリケーションサーバ4は、ネットワーク5を介してクライアント端末2または認証サーバ3との間で、各種データ信号を送受信する送受信部41と、

クライアント端末2へ伝送する伝送文を編集する伝文編集部42と、平文を暗号化する暗号化部44と暗号文を元の平文に復号する復号化部45とを有する暗号処理部43とを備える。このアプリケーションサーバ4は、具体的には、プライベート情報を本人に通知するサービス等を行なう官公庁のホストコンピュータ、警報情報等を関係者に配信するための電力会社のホストコンピュータ、異常情報を関係者に配信するための浄水場の監視コンピュータ、または物流センター内の物流システムを構成するスタッカクレーン、無人搬送車、天井走行車、コンベア等の搬送機器や、各種センサ、制御装置、通信装置等の多様な機器の予防保全データを各リモートメンテナンス企業へ送付する物流センターのホストコンピュータ等である。

【0019】クライアント端末2は、ネットワーク5を介してアプリケーションサーバ4または認証サーバ3との間で、各種データ信号を送受信する送受信部21と、アプリケーションサーバ4へ伝送する伝送文を編集する伝文編集部23と、平文を暗号化する暗号化部25と暗号文を元の平文に復号する復号化部26とを有する暗号処理部24と、バイオメトリクス情報入力装置6がバイオメトリクス情報を読み取るように制御し、バイオメトリクス情報入力装置6が読み取ったバイオメトリクス情報を認証サーバ3に送信するよう制御するバイオメトリクス情報入力装置制御部22とを備える。

【0020】認証サーバ3は、ネットワーク5を介してクライアント端末2またはアプリケーションサーバ4との間で、各種データ信号を送受信する送受信部31と、デジタル証明書を格納するデジタル証明書格納部36と、デジタル証明書格納部36の所定の領域にバイオメトリクス情報を格納させるバイオメトリクス情報登録部32と、クライアント端末2から送信されてきたバイオメトリクス情報がバイオメトリクス情報格納部37に予め格納されたバイオメトリクス情報と台致するか否かを照合する照合部33と、予めデジタル証明書格納部36に格納され、正規なアプリケーションサーバとしてあるいは正規なユーザとして登録してあることを証明するデジタル証明書を発行するデジタル証明書発行部34と、デジタル証明書格納部36の所定の領域に格納された暗号化鍵または復号化鍵を取得する鍵取得部35とを備える。

【0021】また、デジタル証明書格納部36は、所定の領域に、バイオメトリクス情報を格納するバイオメトリクス情報格納部37と、氏名や電子メールアドレスなどX. 509 (ITU-T (International Telecommunication Union Telecommunication standardization: 国際電気通信連合電気通信標準) により勧告されたX. 509) で定められた必須項目を格納する証明情報格納部38及び、暗号鍵を格納す

る格納部39とを有する。

【0022】図2および図3は、本発明における暗号文
伝送時のプログラム処理フローを示す図である。図2に
おいて、送信処理が開始されると、ステップS21で、
クライアント端末またはアプリケーションサーバが有す
る伝送アプリケーションは、伝送する伝文を編成し、ス
テップS22で、暗号ミドルウェア関数呼び出す。図
3に移り、暗号ミドルウェア関数は、ステップS31
で、パラメータで渡された伝送プロトコル種別を判定
し、ステップS32で、伝送プロトコルに対応した公開
鍵暗号方式の暗号ツールを選択する。その後、ステップ
S33で、デジタル証明書から暗号化鍵（送信元である
自分（例えば、クライアント端末またはアプリケー
ションサーバ）の秘密鍵と送信先である相手（送信元がク
ライアント端末の場合はアプリケーションサーバ、送信
元がアプリケーションサーバの場合はクライアント端
末）の公開鍵）を取得し、暗号化処理を行う。そして、
ステップS34で、その暗号化された伝文を送受信部で
伝送処理（送受信）する。

【0023】伝文を受信する場合は、送受信部が伝文を
取り出し、暗号ミドルウェア呼び出す。ユーザ本人が
認証されていない場合は、認証した時点で暗号ミドル
ウェア呼び出す。暗号ミドルウェアではパラメータで渡
された伝送プロトコル種別を判定し、伝送プロトコルに
対応した公開鍵暗号方式の暗号ツールを選択する。その
後、デジタル証明書から復号化鍵を取得し、復号化処
理を行う。その復号化された伝文を受信伝文とする。

【0024】図4は、本発明におけるバイOMETRICS
情報を登録する処理を説明するためのフローチャートで
ある。図4において、バイOMETRICS情報を登録する
処理が開始されると、ステップS41で、バイOMETR
ICS情報入力装置は、ユーザのバイOMETRICS情報、
例えば指紋情報を読み取る。そして、ステップS42
で、読み取った指紋情報等の特徴点情報を抽出等して、
バイOMETRICS情報入力装置に接続されたクライ
アント端末へ上記バイOMETRICS情報を送信する。

【0025】ステップS43で、バイOMETRICS情報
入力装置から送信されたバイOMETRICS情報を受信し
たクライアント端末は、ネットワークを介して認証サー
バへ上記バイOMETRICS情報を送信（転送）する。

【0026】ステップS44で、認証サーバは、クライ
アント端末から送信されたバイOMETRICS情報を受信
する。ステップS45で、バイOMETRICS情報を受信
した認証サーバは、バイOMETRICS情報登録部により
デジタル証明書格納部の所定領域に設けられたバイ
OMETRICS情報格納部に上記バイOMETRICS情報を格
納する。

【0027】このようにして、クライアント端末を利用
する各ユーザのバイOMETRICS情報は、クライアント
端末およびアプリケーションサーバにネットワークを介

して接続された認証サーバのデジタル証明書格納部に
あらかじめ登録される。

【0028】図5および図6は、本発明におけるクライ
アント端末からアプリケーションサーバへ暗号文を伝送
する処理を説明するためのフローチャートである。図5
において、クライアント端末からアプリケーションサー
バへ暗号文を送信する前処理として、ステップS51
で、バイOMETRICS情報入力装置は、上記暗号文を伝
送しようとするユーザのバイOMETRICS情報、例えば
指紋情報を読み取る。そして、ステップS52で、読み
取った指紋情報の特徴点情報を抽出等して、バイOMET
RICS情報入力装置に接続されたクライアント端末へ上
記バイOMETRICS情報を送信する。

【0029】ステップS53で、バイOMETRICS情報
入力装置から送信されたバイOMETRICS情報を受信し
たクライアント端末は、ネットワークを介して認証サー
バへ上記バイOMETRICS情報を送信（転送）する。

【0030】ステップS54で、認証サーバは、クライ
アント端末から送信されたバイOMETRICS情報を受信
する。ステップS55で、バイOMETRICS情報を受信
した認証サーバは、受信したバイOMETRICS情報がバイ
OMETRICS情報格納部に格納されているか否か、す
なわち、正規なユーザとして登録されているか否かを照
合部によって照合する。

【0031】そして、上記照合の結果、ステップS56
で、認証サーバの受信したバイOMETRICS情報とバイ
OMETRICS情報格納部に格納されているバイOMETR
ICS情報とが合致するか否かを判断する。合致した場合
（ステップS56：YES）は、ステップS57で、デ
ジタル証明書発行部により上記暗号文を送送しようと
するユーザが正規なユーザとして登録されている旨のデ
ジタル証明書を、デジタル署名のための暗号化鍵
（例えば、秘密鍵）と共に、正規なユーザとして登録さ
れているか否かを問い合わせたクライアント端末に
対して発行（送信）する。なお、上記暗号化鍵は、鍵取
得部が鍵格納部から取得し、デジタル証明書発行部に
渡す。

【0032】正規なユーザとして登録されているか否か
を問い合わせたクライアント端末は、ステップS58
で、上記デジタル証明書を受信する（前処理終了）。
続いて、伝送処理の説明に移る。ステップS59で、デ
ジタル証明書と共に受信した暗号化鍵で、アプリケー
ションサーバに伝送したい伝文に対してデジタル署名
をする。そして、図6に移り、ステップS60で、上記
デジタル署名をした伝文（平文）自体をあらかじめ入
手したアプリケーションサーバの暗号化鍵（例えば、公
開鍵）で暗号化する。ステップS61で、暗号化した暗
号文を送信先のアプリケーションサーバに対して送信す
る。

【0033】アプリケーションサーバは、ステップS6

2で、上記暗号文を受信し、ステップS63で、あらかじめ認証サーバから入手したユーザの復号化鍵（例えば、公開鍵）で受信した暗号文のデジタル署名を復号化する。

【0034】ステップS64で、暗号文のデジタル署名を復号化したアプリケーションサーバは、上記復号化が正常に行なわれたか否か、すなわち、デジタル署名を行なった暗号化鍵のユーザの復号化鍵で復号化したか否かを判断する。

【0035】そして、上記判断により、正規のユーザからの伝文伝送であるとされた場合（ステップS64：YES）は、ステップS65で、暗号化された伝文自体をあらかじめ入手した復号化鍵（例えば、秘密鍵であり、この復号化鍵は、アプリケーションサーバのデジタル証明書（正規なアプリケーションサーバとして登録されている旨のデジタル証明書）とともに入手可能）で復号化する。なお、正常に復号化されず、正規のユーザからの伝送伝文でないとしてされた場合（ステップS64：NO）は、例えば、上記伝文を破棄し、クライアント端末に対して異常応答をして終了する。

【0036】図7および図8は、本発明におけるアプリケーションサーバからクライアント端末へ暗号文を伝送する処理を説明するためのフローチャートである。図7において、アプリケーションサーバからクライアント端末へ暗号文を伝送する処理が開始されると、前処理としてデジタル証明書を入手する。すなわち、アプリケーションサーバからの伝送先とされたクライアント端末が、ステップS71で、バイOMETRICS情報入力装置に対して、クライアント端末を操作しているユーザのバイOMETRICS情報を入力するように要求する。

【0037】ステップS72で、バイOMETRICS情報を入力するように要求されたバイOMETRICS情報入力装置は、上記ユーザのバイOMETRICS情報、例えば指紋情報を読み取る。そして、ステップS73で、読み取った指紋情報の特徴点情報を抽出等して、バイOMETRICS情報入力装置に接続されたクライアント端末へ上記バイOMETRICS情報を送信する。

【0038】ステップS74で、バイOMETRICS情報入力装置から送信されたバイOMETRICS情報を受信したクライアント端末は、ネットワークを介して認証サーバへ上記バイOMETRICS情報を送信（転送）する。

【0039】ステップS75で、認証サーバは、クライアント端末から送信されたバイOMETRICS情報を受信する。ステップS76で、バイOMETRICS情報を受信した認証サーバは、受信したバイOMETRICS情報がバイOMETRICS情報格納部に格納されているか否か、すなわち、正規なユーザとして登録されているか否かを照会部によって照合する。

【0040】そして、上記照会の結果、ステップS77で、認証サーバの受信したバイOMETRICS情報とバイ

OMETRICS情報格納部に格納されているバイOMETRICS情報とが合致するか否かを判断する。合致した場合（ステップS77：YES）は、ステップS78で、デジタル証明書発行部により上記暗号文を復号化しようとするユーザが正規なユーザとして登録されている旨のデジタル証明書を、暗号文を復号化するための復号化鍵（例えば、公開鍵）と共に、正規なユーザとして登録されているか否かを問い合わせたクライアント端末に対して発行（送信）する。なお、上記暗号化鍵は、鍵取得部が鍵格納部から取得し、デジタル証明書発行部に渡す。

【0041】正規なユーザとして登録されているか否かを問い合わせたクライアント端末は、ステップS79で、上記デジタル証明書を受信する（前処理終了）。続いて、図8を用いて伝送処理について説明する。ステップS80で、あらかじめ入手したデジタル証明書と共に受信した暗号化鍵（例えば、秘密鍵）で、クライアント端末に伝送したい伝文に対してデジタル署名をする。さらに、ステップS81で、上記デジタル署名をした伝文（平文）自体をクライアント端末の暗号化鍵（例えば、公開鍵）で暗号化する。そして、ステップS82で、暗号化した暗号文を送送先のクライアント端末に対して送信する。

【0042】クライアント端末は、ステップS83で、上記暗号文を受信し、ステップS84で、あらかじめ認証サーバから入手したアプリケーションサーバの復号化鍵（例えば、公開鍵）で受信した暗号文のデジタル署名を復号化する。

【0043】ステップS85で、暗号文のデジタル署名を復号化したクライアント端末は、上記復号化が正常に行なわれたか否か、すなわち、デジタル署名を行なった暗号化鍵のアプリケーションサーバの復号化鍵で復号化したか否かを判断する。

【0044】そして、上記判断により、正規のアプリケーションサーバからの伝文伝送であるとされた場合（ステップS85：YES）は、ステップS86で、暗号化された伝文自体をあらかじめ入手した復号化鍵（例えば、秘密鍵であり、この復号化鍵は、アプリケーションサーバのデジタル証明書（正規なアプリケーションサーバとして登録されている旨のデジタル証明書）とともに入手可能）で復号化する。

【0045】なお、上述してきたようなバイOMETRICS情報は、デジタル証明書の運用方法に対応して、必要に応じ、変換テーブルにIDとバイOMETRICS情報との対を待つことにより、デジタル証明書の外部に待つことも可能である。

【0046】また、デジタル証明書内にバイOMETRICS情報を有する場合は、ユーザがクライアント端末で認証する時点において、デジタル証明書を取得済みでありデジタル証明書の有効期限内である時は、クライ

ント端末で入力されるバイOMETRICS情報とデジタル証明書のバイOMETRICS情報を照合することも可能である。

【0047】上述してきたような、アプリケーションサーバを提供するアプリケーションサーバと、ユーザが使用するクライアント端末と、ユーザを認証する認証サーバとが互いにネットワークを介して接続される個人認証システムは、以下のような形態に特に有効である。

【0048】(1) 官公庁における、イントラネットまたはインターネットを介したプライバシー情報などの本人への送付。

(2) 電力会社での電力の系統制御における、イントラネットまたはインターネットを介した警報情報の関係者への配信。

【0049】(3) 浄水場の監視制御における、イントラネットまたはインターネットを介した異常情報の関係者への配信。

(4) 物流センターや工場における、イントラネットまたはインターネットを介した予防保全データのリモートメンテナンス企業への送付。

【0050】上述のように、本発明の実施の形態を、図面を参照しながら説明してきたが、説明したクライアント端末、認証サーバ、およびアプリケーションサーバは、汎用の情報処理装置(コンピュータ)を用いて構成することができる。上記情報処理装置は、CPU(中央処理装置)、メモリ、入力装置、出力装置、外部記憶装置、媒体駆動装置、およびネットワーク接続装置を備え、これらはバスにより互いに接続されている。

【0051】メモリは、例えば、ROM(Read Only Memory)、RAM(Random Access Memory)等を含み、処理に用いられるプログラムとデータを格納する。CPUは、メモリを利用してプログラムを実行することにより、必要な処理を行う。

【0052】入力装置は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、ユーザからの指示や情報の入力に用いられる。出力装置は、例えば、ディスプレイ、プリンタ、スピーカ等であり、ユーザへの問い合わせや処理結果の出力に用いられる。

【0053】外部記憶装置は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。情報処理装置は、この外部記憶装置に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリにロードして使用することができる。また、外部記憶装置は、登録データ、登録データの種別、ID番号等を保存するデータベースとしても用いることができる。

【0054】媒体駆動装置は、可搬記録媒体を駆動し、その記録内容にアクセスする。可搬記録媒体としては、メモリカード、フロッピーディスク、CD-ROM(Compact Disk Read Only Mem

ory)、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。管理者は、この可搬記録媒体に上述のプログラムとデータを格納しておき、情報処理装置は、必要に応じて、それらをメモリにロードして使用することができる。

【0055】ネットワーク接続装置は、任意のネットワーク(回線)を介して外部の装置と通信し、通信に伴うデータ変換を行う。また、情報処理装置は、必要に応じて、ネットワーク接続装置を介して上述のプログラムとデータを外部の装置から受け取り、それらをメモリにロードして使用することができる。

【0056】すなわち、本発明は、以上に述べた実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲内で種々の構成または形状を取ることが出来る。

【0057】

【発明の効果】本発明によれば、アプリケーションサーバとクライアント端末との間で暗号文を伝送する場合に、認証サーバが格納しているデジタル証明書で照合を行うため、伝文伝送の安全性を高める事ができる。

【0058】また、本発明によれば、デジタル証明書を認証サーバからダウンロードする場合も、従来必要とされていたIDやパスワード等を入力を行わずに、バイOMETRICS情報を用いた認証により自動で認証サーバからデジタル証明書をダウンロードすることを可能となる。

【0059】また、本発明によれば、ユーザのID情報の変換テーブルを有することにより、バイOMETRICS情報を有しないデジタル証明書であっても同様の処理が可能となる。

【0060】すなわち、本発明によれば、アプリケーションサーバとクライアント端末との間のネットワークの情報は、暗号化され、クライアント端末における認証によりアクセス権限が確認される。これにより、盗聴、改ざん、なりすましを防止することができ、インターネットやイントラネットに接続した任意のクライアント端末からいつでも高い安全性でアプリケーションサーバの情報を取得できる。さらに、取得もユーザから要求するだけでなく、アプリケーションサーバから随時送付できる。

【0061】また、本発明によれば、バイOMETRICS情報を用いた認証により、IDやパスワード等の入力のわずらわしさを回避することができる。

【図面の簡単な説明】

【図1】本発明の個人認証システムの機能ブロック図である。

【図2】本発明における暗号文伝送時のプログラム処理フローを示す図(その1)である。

【図3】本発明における暗号文伝送時のプログラム処理フローを示す図(その2)である。

【図4】本発明におけるバイオメトリクス情報を登録する処理を説明するためのフローチャートである。

【図5】本発明におけるクライアント端末からアプリケーションサーバへ暗号文を伝送する処理を説明するためのフローチャート（その1）である。

【図6】本発明におけるクライアント端末からアプリケーションサーバへ暗号文を伝送する処理を説明するためのフローチャート（その2）である。

【図7】本発明におけるアプリケーションサーバからクライアント端末へ暗号文を伝送する処理を説明するためのフローチャート（その1）である。

【図8】本発明におけるアプリケーションサーバからクライアント端末へ暗号文を伝送する処理を説明するためのフローチャート（その2）である。

【符号の説明】

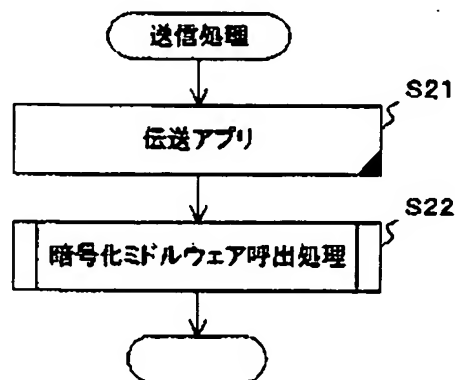
- 1 個人認証システム
- 2 クライアント端末
- 3 認証サーバ
- 4 アプリケーションサーバ4
- 5 ネットワーク
- 6 バイオメトリクス情報入力装置

- * 2 1 送受信部
- 2 2 バイオメトリクス情報入力装置制御部
- 2 3 伝文編集部
- 2 4 暗号処理部
- 2 5 暗号化部
- 2 6 復号化部
- 3 1 送受信部
- 3 2 バイオメトリクス情報登録部
- 3 3 照合部
- 3 4 デジタル証明書発行部
- 3 5 鍵取得部
- 3 6 デジタル証明書格納部
- 3 7 バイオメトリクス情報格納部
- 3 8 証明情報格納部
- 3 9 鍵格納部
- 4 1 送受信部
- 4 2 伝文編集部
- 4 3 暗号処理部
- 4 4 暗号化部
- 4 5 復号化部

*

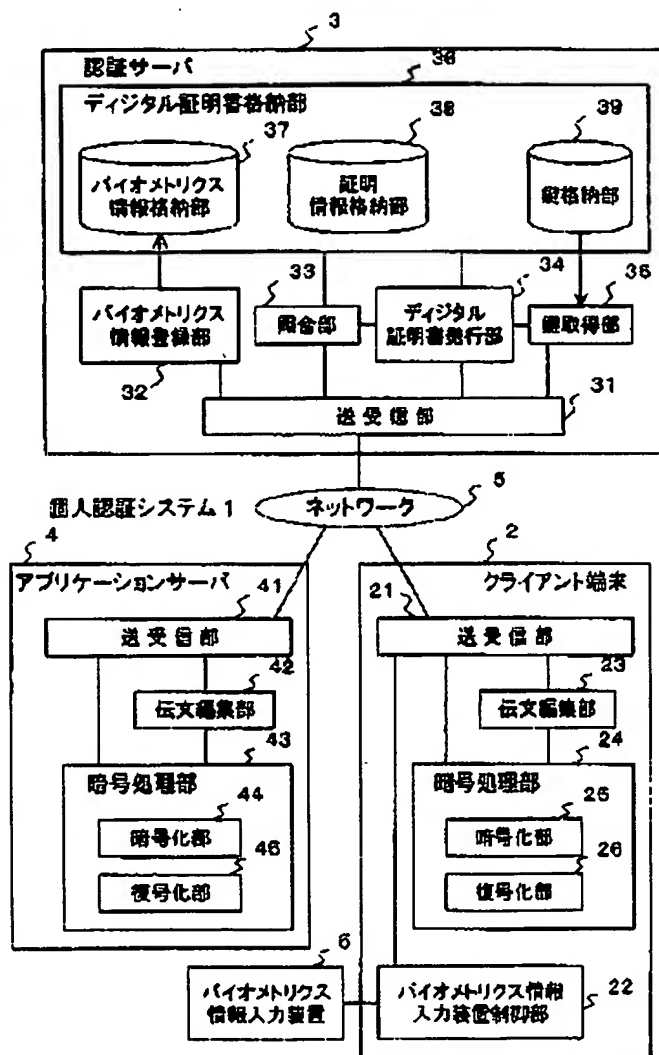
【図2】

本発明における暗号文伝送時の
プログラム処理フローを示す図（その1）



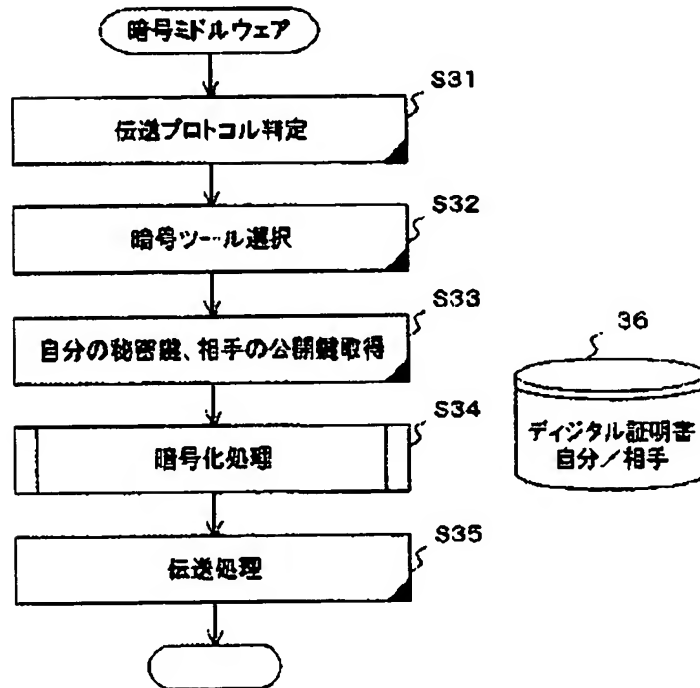
【図1】

本発明の個人認証システムの機能ブロック図



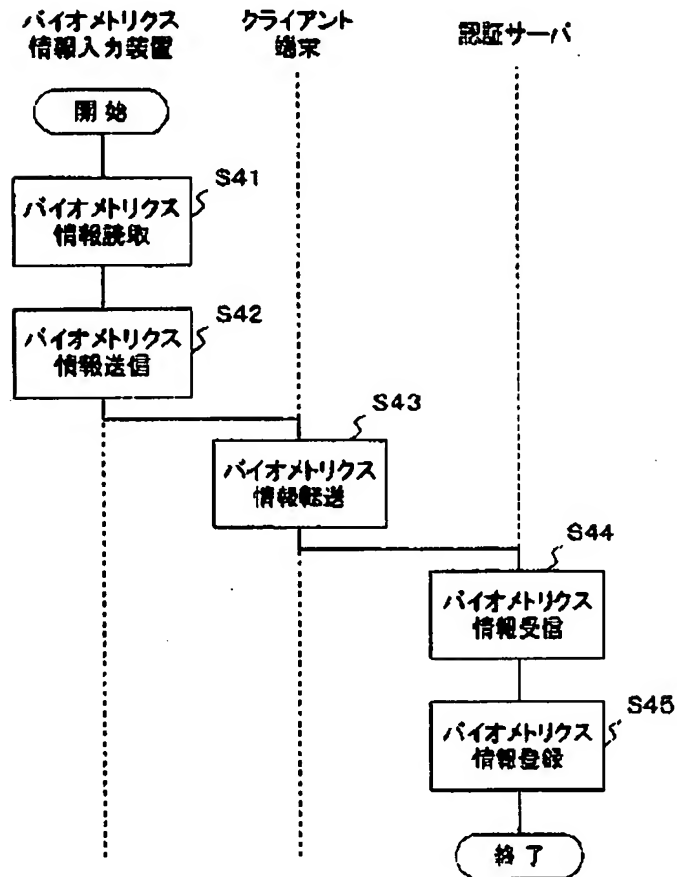
〔図3〕

本発明における暗号文伝送時の
プログラム処理フローを示す図(その2)



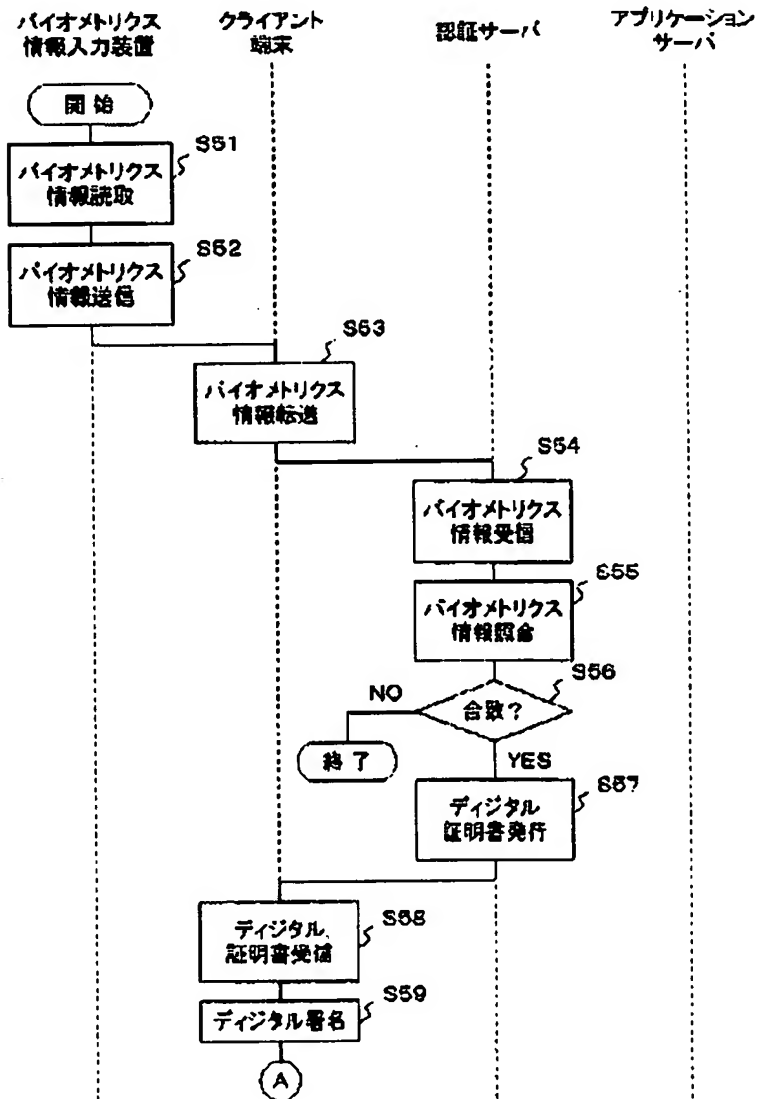
〔図4〕

本発明におけるバイOMETRICS情報を登録する処理を説明するためのフローチャート



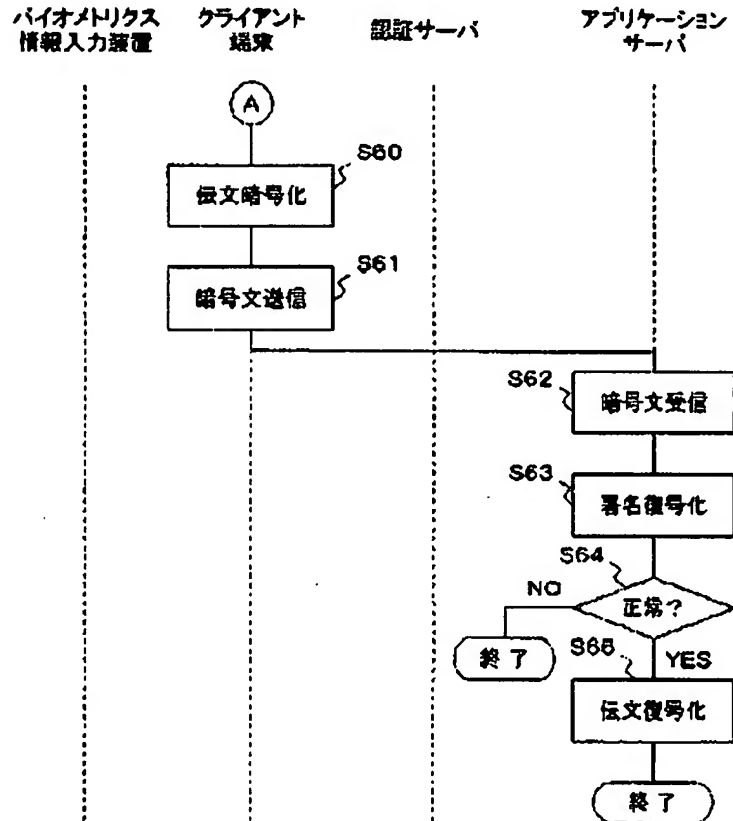
【図5】

本発明におけるクライアント端末からアプリケーションサーバへ
暗号文を送送する処理を説明するためのフローチャート(その1)



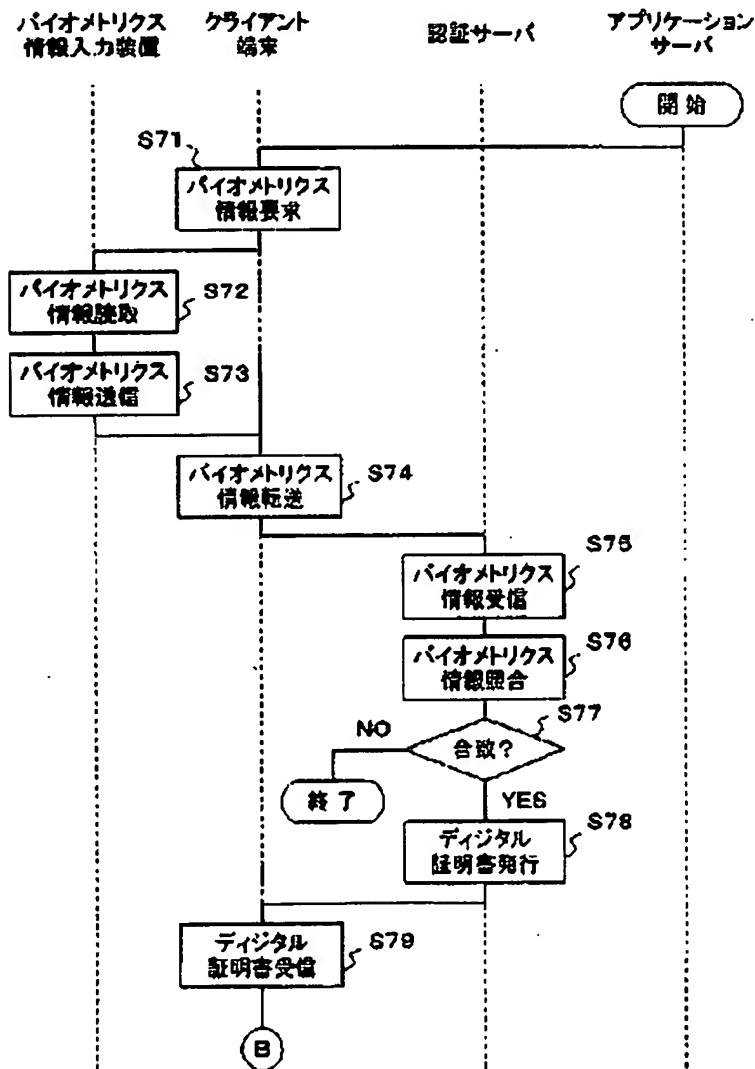
【図6】

本発明におけるクライアント端末からアプリケーションサーバへ
暗号文を伝送する処理を説明するためのフローチャート(その2)



【図7】

本発明におけるアプリケーションサーバからクライアント端末へ
暗号文を送送する処理を説明するためのフローチャート(その1)



【図8】

本発明におけるアプリケーションサーバからクライアント端末へ
暗号文を伝送する処理を説明するためのフローチャート(その2)

